PATENT APPLICATION TRANSMITTAL LETTER (Large Entity)	Docket No. 00280552AA

j 639 U.S. PTO

TO THE ASSISTANT COMMISSIONER FOR PATENTS

01/24/00

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Rudolf M. Bolle, Nalini K. Ratha and Andrew Senior

For: **IMPROVEMENTS TO A COMBINED FINGERPRINT ACQUISITION AND CONTROL DEVICE**

Enclosed are:

☐ Certificate of Mailing with Express Mail Mailing Label No.
☒ **seven informal** sheets of drawings.
☐ A certified copy of a   application.
☒ Declaration   ☒ Signed.   ☐ Unsigned.
☒ Power of Attorney
☐ Information Disclosure Statement
☐ Preliminary Amendment
☐ Other:

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate		Fee
Total Claims	27	- 20 =	7	x	$18.00	$126.00
Indep. Claims	4	- 3 =	1	x	$78.00	$78.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$690.00
					TOTAL FILING FEE	$894.00

☐ A check in the amount of   to cover the filing fee is enclosed.
☒ The Commissioner is hereby authorized to charge and credit Deposit Account No.   50-0510
as described below. A duplicate copy of this sheet is enclosed.
  ☒ Charge the amount of $894.00   as filing fee.
  ☒ Credit any overpayment.
  ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance,
  pursuant to 37 C.F.R. 1.311(b).

Dated: January 23, 2000

Signature

Elizabeth W. Cook
Registration No. 39,640
Whitham, Curtis & Whitham
11800 Sunrise Valley Drive, Suite 900
Reston, Virginia 20191

703-391-2510

CC:

IMPROVEMENTS TO A COMBINED FINGERPRINT ACQUISITION AND CONTROL DEVICE

DESCRIPTION

BACKGROUND OF THE INVENTION

5

Cross Reference to Related Application

This application is related to copending U.S. application serial number 09/080,322 to Andrew Senior, filed on May 15, 1998.

Field of the Invention

10 The present invention generally relates to the field of computer input devices and, more particularly, to pointing devices, fingerprint acquisition devices, and secure fingerprint acquisition.

Background Description

Most common computer operating systems presently incorporate windowing in presenting information to users. Common examples of such

15 software, often referred to as graphical user interfaces (GUIs), include Microsoft Corporation's Windows series and Apple Corporation's Mac OS. In such computer systems, a spatial metaphor is used to present information.

Some kind of pointing device is almost indispensable for the use of such a computer interface. Beginning with the mouse, a wide variety of

20 pointing devices have been introduced, including trackballs, touchpads, and a

variety of mechanical pointers. An example of such a pointing device is described in U.S. Patent No. 5,489,900 to Cali et al. for "Force Sensitive Transducer for Use in a Computer Keyboard."

5   Such pointing devices which are alternative to the mouse are especially desirable for use with mobile computers. The users of such mobile computers often do not have available the large, flat space necessary for operating the traditional mouse.

Hence, a flood of pointing devices has been introduced in recent years, adapted for use with mobile computers. Each such device has advantages and
10   disadvantages, allowing for a range of alternatives which may be adapted to a variety of usage scenarios and personal preferences.

It would therefore be desirable to provide a fingerprint authentication device capable of allowing user pointing, which is compact enough for incorporation into a mobile computer or other portable electronic device. Such
15   a device would allow for user authentication without separate, active intervention by the user.

Pending application U.S. serial no. 09/080,322 employs the steps of viewing the fingerprint as an elliptical region, using this view to find rotation in the plane of the scanner, and finding the principle axes of this region. The
20   contents of U.S. serial no. 09/080,322 are hereby incorporated by reference. However, it is found that when pressure is light, only the very tip of the finger is used, or when the finger is at the edge of the scanning area, the principal axis of the on pixels does not correspond to the principal axis of the finger tip, as a result the reliability of this scanning method could be improved.

25   Fingerprint matching is a well-established and reliable method of identifying individuals. As such, it provides a good method for authentication of the identity of a person for such purposes as enabling use of equipment, access to data, and the authorization of transactions. In recent years, powerful

YO999-270

processors and new algorithms, coupled with a variety of new, "livescan" fingerprint scanning devices, have enabled the automatic verification of fingerprints on small computer platforms.

5

The incorporation of such authentication devices would be particularly useful for notebook, laptop and other mobile computers, as well as in other portable electronic devices such as cellular telephones, personal digital assistants, etc. Mobile computers are more likely than desktop computers to be present in unsecured areas where unauthorized individuals might attempt to use or access the computer. Because users of such mobile computers often

10

have confidential or proprietary information stored in these computers, such users have a strong interest in maintaining the security of their computers. Similarly, mobile phones are carried in public and are easily stolen, presenting a considerable financial risk in unauthorized use.

Nevertheless, existing security systems for such computers and phones

15

require intentional, active intervention by the user, such as entering passwords or using key locks. The inconvenience of such frequent activity, in conjunction with the user's fears of misplacing or forgetting the key or password, often result in users ignoring available security systems.

Biometrics systems that are not designed with the proper safeguards

20

are vulnerable to a number of attacks which can bypass or invalidate the security derived from such a system. One such category of attack is the replay attach. In this situation, data captured at a previous verification session is recorded by an eavesdropper, and replayed to the system layer when claiming authorization. Such attacks can be prevented with this device in a number of

25

ways.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide new and improved methods of calculating the parameters previously described, and of using the parameters calculated.

5   It is further an object to provide an improved method to calculate rotational information for a fingerprint.

In describing the inventive system, it must be kept in mind that the scanner is imaging the interface between the finger and the scanner. As has been described before, this image will vary depending on the position and

10   rotation of the fingertip. It is simple to work out where the fingertip is in contact with the scanner, by looking at which area of the image displays a fingerprint, but it is more difficult to determine the rotation of the finger with respect to the scanner.

BRIEF DESCRIPTION OF THE DRAWINGS

15   The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a perspective illustration of a mobile computer100 incorporating a combined fingerprint image scanner and pointing device

20   according to a the present invention;

Figure 2 is an illustration of the usable fingerprint scanner surface 210 of scanner 130 of Figure 1;

Figure 2a is an illustration of a "tiled" fingerprint scanner using a row of small fingerprint scanners;

25   Figure 2b is an illustration of a "tiled" fingerprint scanner using set of

smaller fingerprint scanners, in a two-dimensional array;

Figure 3 shows an example of comparison of two consecutive fingerprint images according to this invention;

Figure 4 is a flow diagram of the authentication process in general;

5   Figure 5 is a flow diagram showing specific details of the authentication process; and

Figure 6 is a flow diagram showing additional steps which may be added to the authentication process.

DETAILED DESCRIPTION OF A PREFERRED
10   ## EMBODIMENT OF THE INVENTION

When comparing two fingerprint images of the same finger acquired from an imaging device (or indeed different capture systems), the patterns in the fingerprints may be different for a number of reasons, including plane rotation: the rotation of the finger about an axis perpendicular to the plane of

15   the scanner. Such a rotation would cause features in the images to rotate about the axis of rotation. Other processes will cause the features to move about in other ways such as translation.

In operation, the invention may be used as a security device for a mobile computer as shown in Figure 1. In Figure 1 there is shown a computer

20   100, having as screen 110 and keyboard 120. Computer 100 is shown having a combined fingerprint scanner and pointing device scanner130 according to the present invention. A pair of optional control buttons 140 are also shown. Control buttons 140, may be used , for example, as substitutes for the buttons of a mouse. It should be noted that mobile computer 100 could be

25   programmed to recognize some control signals such as a corresponding predetermined series of finger taps of short duration as representing the same

functions as depressing each optional control button 140, whether or not optional control buttons 140 are present.

The preferred embodiment of the invention uses a compact, thin, flat scanner 130. The presently preferred choice of such a scanner 130 is that of a

5 semiconductor fingerprint sensor, such as that described by Taikoe in U.S. Patent 4,353,056. While such a semiconductor scanner 130 is presently preferred for use in conjunction with mobile computers, a wide variety of choices of mechanisms for fingerprint acquisition by scanner 130 may be used in accordance with the present invention. Optical scanning may be used either

10 by frustrated total internal reflection, holographic elements or by conventional reflected light imaging. Similarly, a variety of electrical or electromagnetic scanners, semiconductor or otherwise, may be used, which utilize either capacitive or inductive scanning. Ultrasound imaging of the fingerprint might also be used. The present invention is compatible with any choice of

15 fingerprint scanners which permit digital acquisition or interpretation of the fingerprint image.

The preferred embodiment of the present invention would require a scanner 130 several times larger than that of currently available semiconductor fingerprint scanners, to allow enough motion of the finger to allow

20 unrestricted control pointing functions. Such currently available semiconductor fingerprint scanners are sized solely for static presentation of fingerprints for authentication scanning purposes.

The semiconductor scanners being smaller in size (less than half the size of a normal average finger), a large scan area can be achieved by tiling a

25 set of small fingerprint scanners to form a large scanning area 130 as shown in Figures 2a and 2b. The small scanners can be tiled in either a one-dimensional array 270, as shown in Figure 2a, or as a two-dimensional array 280 as shown in Figure 2b.

The need for such a large scanner 130 is best understood relative to Figure 2. Figure 2 shows a diagram of a fingerprint scanner surface 210 with an acquired fingerprint image 220. Fingerprint scanner surface 210 corresponds to the functional area of scanner 130. The portion of the surface

5   area of scanner 130 which comprises scanner surface 210 depends upon the function characteristics of scanner 130, which may vary dependent upon the image acquisition method employed by scanner 130.

The presently preferred embodiment of the present invention calculates a center-of-area or centroid 230 of fingerprint image 220. Centroid 230 has an

10   associated two dimensional coordinate relative to fingerprint scanner surface 210, which in Figure 2 is represented as an x-coordinate 240 and a y-coordinate 250. The choice of coordinate systems is arbitrary, and may be chosen to facilitate computations related to the specific or general application of the device according to the present invention. This calculation is performed

15   with each fingerprint image collected.

Having calculated a coordinate pair representative of fingerprint image 220, this coordinate pair allows scanner 130 to be used as a two-dimensional pointing device, in a manner well known in the prior art. For example, the coordinate of the scanner may be remapped to screen coordinates, so that the

20   absolute finger position on scanner 130 relative to scanner surface 210 corresponds to an absolute screen position, just as with an electronic pen tablet. With such a remapping implementation, it is preferable to allow a margin of about half of a finger's width, mapping the area within such a margin to the screen area, to allow the user to easily point to any position on

25   the screen with the centroid 230 of fingerprint image 220.

Alternatively, any movement of the finger in contact with scanner 130 would continuously change successive coordinates of centroid 230, allowing calculation of relative motion of acquired fingerprint images 220. This relative

motion may be remapped to the motion of the cursor on the screen, in a manner similar to that of a joystick.

To determine the relative rotation of the finger between the two images, it is sufficient to find the rotation of the features between the images.

5   This can be done by some feature extraction and alignment process, but a simple method of doing this is by finding image correlations. In the preferred embodiment of this method, small regions of one image are considered, and the most similar region in the other image is searched for. The motion of the first region to the second region is ambiguous, because of errors in the

10   measurement process, but by considering a large number of regions with sufficient detail to limit the number of matching areas, a consensus will be reached, and the parameter of this motion can be considered to correspond to the motion of the finger.

In practice, a number of simplifying assumptions can be made to make

15   this process efficient. In particular, if the images are gathered sequentially from a scanner with a high frame rate, the motions of the regions will be small. Thus, if a rectangular region of pixels is considered in one image, parallel to the axis, only nearby rectangular regions need to be searched. Further, since the rotation is small, the rectangular region will be translated to

20   a rectangular region which is close enough to the axes to appear very similar to a similar axis-parallel rectangle. Thus, the search need only be conducted over nearby axis-parallel rectangles of the same size as the original region. The search is conducted to find the most similar such rectangle in the search region, using a similarity metric such as normalized correlation coefficient.

25   The most similar region being found, its displacement with respect to the region in the original image can be calculated. Note that in this situation, it is unclear whether this displacement arose from pure translation, or from translation and rotation combined. However, the set of pairs of values of

in the new image, the displacement resulting in the highest correlation coefficient is considered to be the new location of the selected area. The displacement of the matching region is noted, and entered as a vote in a translation table 360. After comparing many such areas of the original image, many "votes" have been entered in the table, as shown, and by picking the displacement with the largest number of votes, the aggregate translation of the fingerprint can be estimated.

If the rotation and translation are to be estimated, the voting table will have three dimensions (x, y, theta) and any given translation calculated for an image area, will correspond to many triplets of values in the table. A vote is entered in each box in the voting table consistent with the translation measured At the end, the box with the highest number of votes is chosen, and the translation, rotation parameters are read off.

In practice these translation parameters represent translation due to the finger being translated across the surface, and the translation measured by a method such as the centroid method described previously will include components due to this translation but also due to the pitch and roll rotations of the finger. A variety of methods of combining these control parameters can be used to extract final control parameters suitable for controlling the computer, decoupled in a way intuitive for a given application or user. One of the aspects of this invention is to link pointing and authentication devices through fingerprints. Several preboot authentication methods using passwords are incorporated in the systems today using BIOS passwords.

The authentication process is broadly shown in the flow chart in Figure 4. At the start 401, the user is prompted 402 for authentication. If authentication is positive 403, the boot process is complete 404. However, if the authentication is negative, then the system cycles through the prompting steps 401 again until it is verified that three attempts 405 have been made to

YO999-270

{translation, rotation} consistent with this observed displacement can be found.

By considering many such displacements, a consensus on the true translation and rotation can be found. One mechanism for doing this is to use the Hough transform, where the space of translations x rotations is divided into bins. Each displacement causes votes for all the bins with which it is consistent, and after all regions have voted, the bin with the highest number of votes is deemed to represent the true rotation and translation.

Optionally, a Hough transform based alignment of two fingerprint minutia templates can be used as presented in the following reference and is incorporated in its entirety. In this case the regions of interest in a fingerprint image 303 are chosen by a fingerprint feature extraction algorithm. N.K. Ratha, K. Karu, S. Chen, and A. Jain, "A Real-Time Matching System for Large Fingerprint Databases" , IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 18, No. 8 August 1996, pp. 799-813.

An example of finding the translation parameters for the movement between two consecutive images acquired from a fingerprint scanner is shown in Figure 3. The diagram shows image 301 acquired from a fingerprint scanner, showing the image, 302 of a fingerprint. At some subsequent time, a new image 331 is acquired from the scanner with a new image of the fingerprint 332 which may have moved relative to its position in the previous image 302. One method for determining this displacement is to observe the motions of segments of the image. In a preferred embodiment, sections 303 of the fingerprint image are chosen (possibly at random or by some algorithm). The corresponding areas 333 of the fingerprint 331 are sought. This search is carried out by one of a number of inexact pattern matching algorithms, such as the method of correlation. In the correlation method, for some given area in the original fingerprint, it is compared with image areas around that location

achieve authentication. After three attempts the computer is shut down 406.

Using fingerprints for authentication poses new problems. Fingerprint authentication systems are vulnerable to new types of attacks which can bypass the security described in Figure 4. One example of this is the replay

5   attack using stored fingerprints. In this case, a stored fingerprint image is replayed to the authentication system. The invention described herein can be used to circumvent such attacks in a number of ways. First, consider the case when a still image has been eavesdropped or captured from some other source, such as the lifting of a latent print. When replayed this image will be seen by

10   this invention to be static, with the derived pose parameters unchanging and can be rejected as a replay attack.

Now, suppose that a video sequence of a fingerprint has been recorded. The computer system can prompt the user to move his or her finger in a particular manner (e.g. "Move left", "press harder", "rotate counterclockwise",

15   etc.). Such prompts can be verified by observing the derived parameters when a live user presents a finger to be scanned and makes the requested gesture. But for a simple replay attack, the image sequence is predetermined and cannot respond to prompts, and so exposed as a replay attack. In the case of several small fingerprint scanners as in Figure 2a or 2b, there are many other

20   ways of achieving this step. For example, the user can touch the different tiles in a particular sequence and remember it as the password. This sequence of touches can be using either a single finger or multiple fingers with the finger used for each touch also being part of the "password".

The inventive system combats replay attacks with the steps shows in

25   the flow chart of Figure 5. Figure 5 is a flow diagram for the operation of validating a user by prompting the user for a fingerprint 501, and by requiring the user to make finger movements (on the scanner or by reapplication of the finger to the scanner) to prevent replay attacks. As can be see, the user is

YO999-270

prompted for a fingerprint 501. After waiting for the fingerprint 502 , the system determines if it matches the template 503. If the template is not matched then the user is rejected 504. If the template is matched, then the user is prompted for the finger movement 505. The movement can be chosen at

5   random by the computer and the movement request will be unknown to the user until the time of request. After waiting for the user's movement 506, a determination is made as to whether the gesture matches the prompt 507. If not, the user is again rejected 504. Following step 507, a determination is made in step 508 as whether enough gestures were made. In some applications

10   more than one gesture will be required. If enough gestures have not been made the system return to block 505 and prompt the user for another finger movement. Once enough gestures have been made the user is accepted as shown in block 509.

This system can also be used as a kind of password which protects the

15   user from replay attacks, where a sophisticated computer program could mimic the gesture requested. In this case, the user chooses a sequence of simple gestures to be presented to the device, and the system asks for the sequence to be executed at verification time. The sequence is secret so cannot be simulated by an impostor, and can be changed in the event of an

20   eavesdropper recording one such sequence, thus overcoming one of the limitations of biometrics - that they are unchangeable and cannot be revoked whenever some one else has a copy.

An alternative authentication process is shown in the flow chart of Figure 6. As can be seen, this process includes the same steps shown in

25   blocks 501 through 504 of Figure 5. The diagram shows the operation of validating a user by prompting for a "gestural password" where in addition to presenting the finger to the scanner, the user must move the finger in a predefined, user-dependent, secret manner to prove that the user possesses the

secret knowledge of this sequence. Once a matched template is found 503, the user is prompted for a finger motion "password" 605. The user has stored a motion previously. The user may change her finger motion password at anytime for increased security. Following the prompt for a password 605, the system awaits the user's movement 606, then makes a determination as to whether the movement matches the expected "password" 607. If a match is made the user is accepted 608, otherwise the user is rejected 504.

The inventive method has a number of uses for the information acquired from the sensor. The position information can be used as input to a gesture recognizer, or a character recognizer, whether handprint, cursive handwriting or a symbolic code like graffiti® . Without a specially constructed code, drawing such gestures on a standard fingerprint scanner would be difficult because of the size, but a number of sensors could be tiled together in a rectangular array to allow sensing over a wider area, making input of positional information for pointing or gesture input more easy.

An individual using the system might wish to tune parameters of the system to suit their own dexterity and preferences. In particular, parameters affecting the method and sensitivity for button click actions, and speed of cursor motion are customizable in the system. Since the system can identify the user with a fingerprint, after initial set-up, a user's customization settings can be selected automatically. An optional aspect of the invention is an initial calibration step for calibrating the pointing device. If the device is to be used as a pointing and authentication device, the user must be enrolled by a process in which the fingerprint and the "gestural password" are stored in the system.

While the invention has been described in terms of a single preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.

YO999-270

CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1   1.   A method for authenticating a user for input of control information for
2   an electronic device, said method comprising:
3   acquiring through a scanner at least two fingerprint images of a finger;
4   and
5   extracting from each said fingerprint image at least one contact
6   parameter, calculated by computing correlations between image attributes in
7   each said fingerprint image.

1   2.   A method as in claim 1, wherein said contact parameter is rotation.

1   3.   A method as in claim 1, wherein said contact parameter is translation.

1   4.   A method as in claim 3, further comprising calculating pitch and roll
2   rotations.

1   5.   A method as in claim 1, further comprising computing correlations of a
2   single portion of said image.

1   6.   A method as in claim 1, further comprising computing correlations
2   between a multiplicity of small regions.

1   7.   A method as in claim 1 further comprising determining the rate of
2   change of some control parameter where a rotation or translation of said finger

3   relative to a reference position is used to determine the rate of change of some

4   control parameter of the computer.

1   8.   A method as in claim 7 further comprising, measuring a pitch and roll

2   rotation, and using to control the position of a cursor in the computer.

1   9.   A method as in claim 7 wherein said the reference position is the

2   position at which contact with the scanner is first registered, the reference

3   point being reset every time the finger reestablishes contact with the scanner.

1   10.   A method as in claim 1 further comprising comparing successive, and

2   possibly consecutive, images taken from a single period of contact of said

3   finger with said scanner.

1   11.   A method as in claim 1 wherein at least one said fingerprint images is

2   a reference image captured previously.

1   12.   A method as in claim 11 wherein the reference image is labeled with

2   known rotation information.

1   13.   A method as in claim 12 further comprising prompting the user to

2   present the finger at known rotations in an enrollment stage to provide said

3   known rotation information

1   14.   A system for authenticating a user and for input of pointing

2   information for a computer, said system comprising:

3   a fingerprint image acquisition scanner for acquiring a fingerprint

4   image of a finger; and

5   an image processor for extracting from said fingerprint image at least

6   one contact parameter other than any optional authentication status data for

7   said fingerprint image.

1   15.   A system as in claim 14 wherein a multiplicity of variations in each

2   of said contact parameters are used to verify an acquisition of data in real time

3   from a live user.

1   16.   A system as in claim 15 wherein a user is directed by the system to

2   follow through on any combination of a multiplicity of prompts including:

3   change a position of, add pressure to contact or rotate said finger from which a

4   fingerprint image is acquired and wherein said multiplicity of prompts are

5   verified by the system to ensure that the data is being generated at the time of

6   direction.

1   17.   A system as in claim 14 where the user is prompted to enact a

2   sequence of finger actions previously registered by the user as a "password"

3   for the device.

1   18.   A system as in claim 14 wherein a motion of the finger tip is

2   interpreted as a gesture for recognition by a gesture engine, for instance

3   character recognition or a Graffiti like engine.

1   19.   The system of claim 14, further comprising:

2   a feature extraction processor for extracting representative features

3   from said fingerprint image;

4   a memory for storing representative features of at least one

5   authorized user; and

6   a feature comparison processor for comparing said stored

7   representative features with said extracted representative features, and

8   generating authentication status data therefrom.

1   20.   A system as in claim 19 wherein an identity of a user is used to set

2   customized features of the computer.

1   21.   A system as in claim 19 where the identity of said user is used to set

2   customized parameters of the pointing device.

1   22.   A system for imaging a fingerprint for input of control information

2   for an electronic device, said system comprising:

3   a fingerprint image acquisition scanner for acquiring a fingerprint

4   image of a finger; and

5   an image processor for extracting from said finger print image at

6   least one contact parameter, representing the angle of the finger in relation to

7   the scanner, where said angle is calculated by computing correlations between

8   image attributes an two or more images acquired from scanners.

1   23.   A system for authenticating a user and for input of pointing

2   information for a computer, said system comprising:

3   a multiplicity of fingerprint image acquisition scanners providing a

4   large input surface for acquiring a fingerprint image of a finger; and

5   an image processor for extracting from said fingerprint image at

6   least one contact parameter other than any optional authentication status data

7   for said fingerprint image.

1   24.   A system as in claim 23, where the scanner consists of a one-

2   dimensional array of small fingerprint scanners.

1   25.   A system as in claim 24, where the scanner consists of a two-

2   dimensional array of small fingerprint scanners.

1   26.   A system as in claim 17, where the "password" is a sequence of

2   touching individual small fingerprint scanners in a specific order with the

3   same finger.

1   27.   A system as in claim 26, where the password is a sequence or

2   touching individual small fingerprint scanners in a specific order, with more

3   than one finger being used in the sequence either serially or in parallel.

COMBINED FINGERPRINT ACQUISITION
AND CONTROL DEVICE

ABSTRACT OF THE DISCLOSURE

The present invention combines the functionality of a computer

5   pointing device with a fingerprint authentication system. In the preferred

embodiment, by regularly scanning fingerprints acquired from the pointing

device touch pad, fingerprint features may be extracted and compared to

stored data on authorized users for passive authentication. Furthermore,

calculations based upon the acquired fingerprint images and associated

10 features allows the system to determine six degrees of freedom of the finger,

allowing the user to control a variety of functions or to manipulate a three-

dimensional model or virtual reality system.

YO999-270
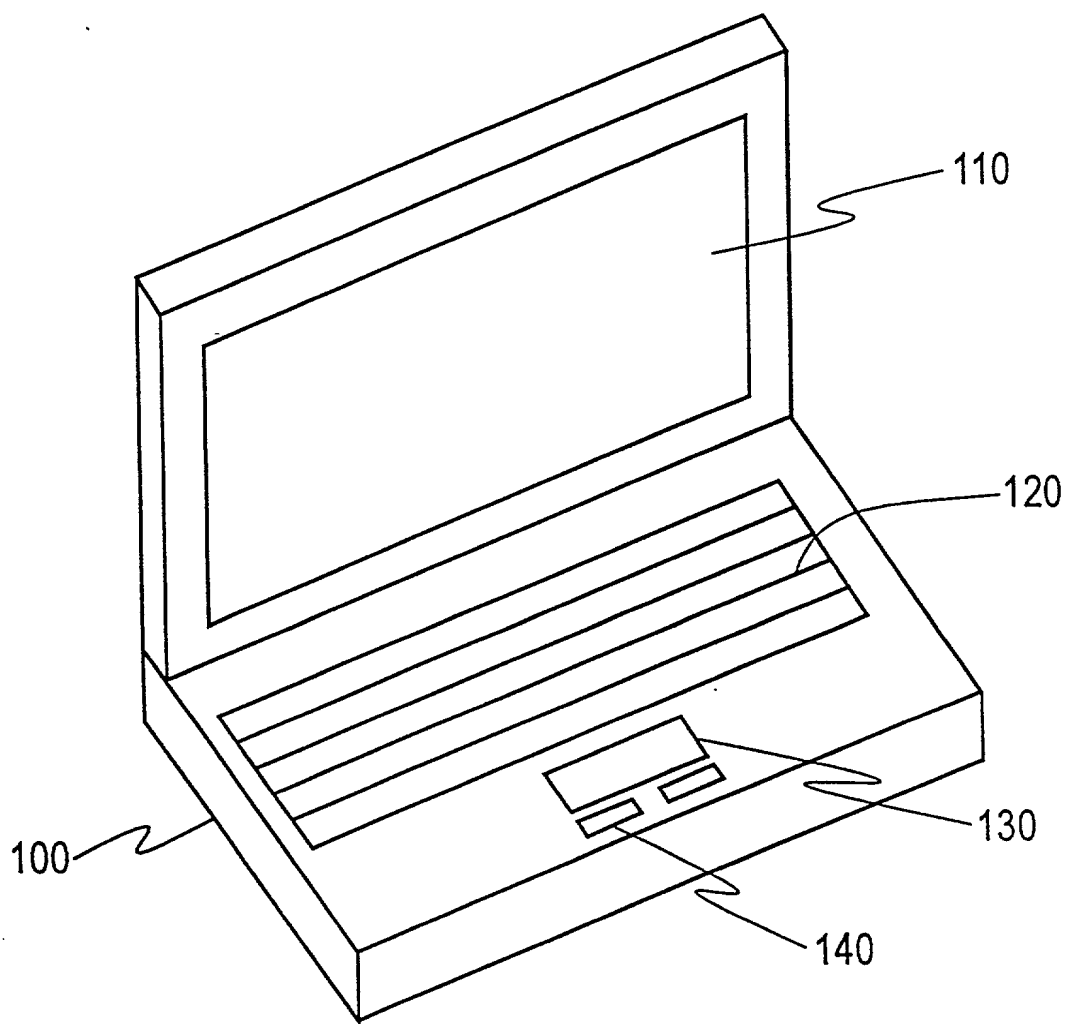
Fig. 1
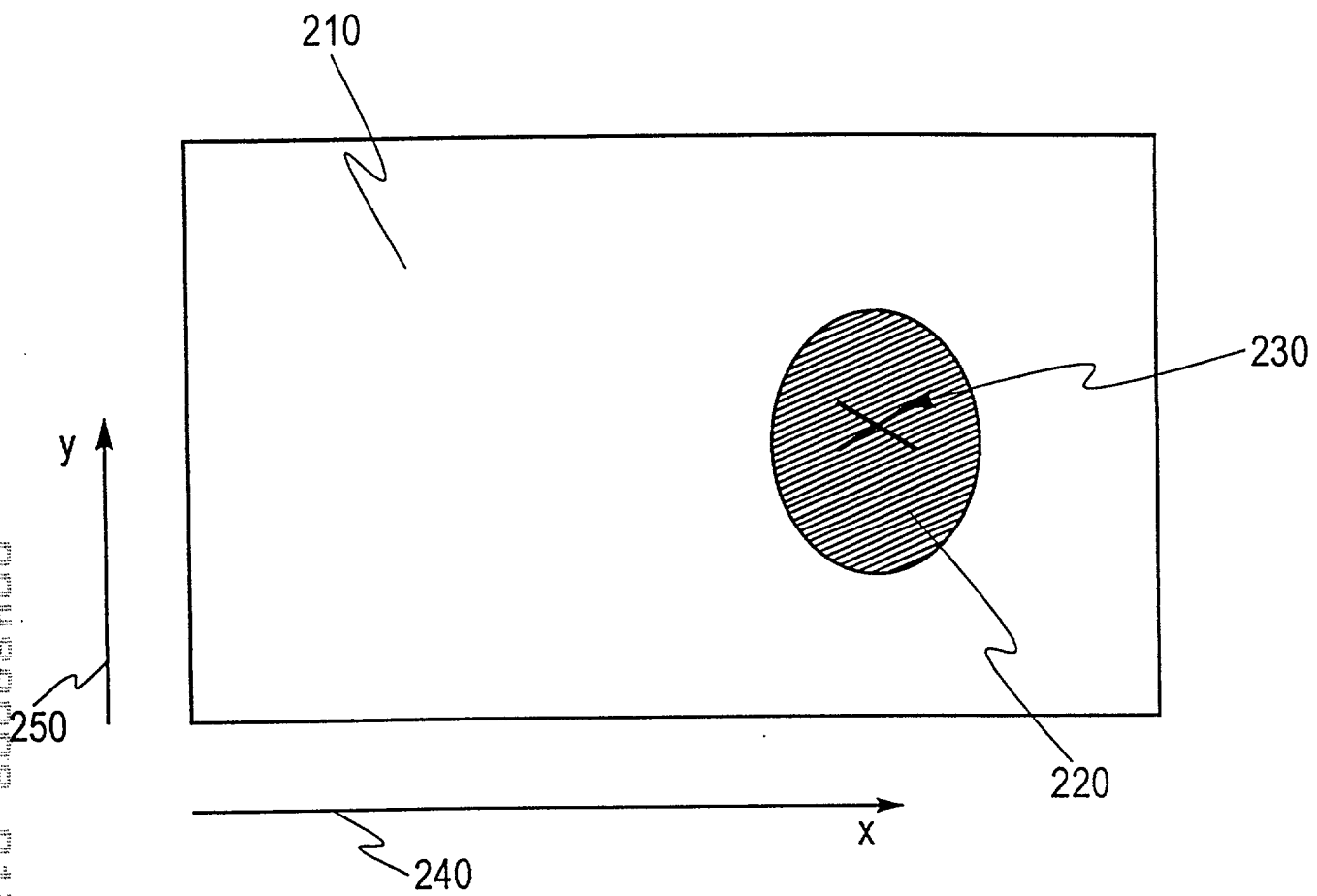
Fig. 2

130	130	130	130
130	130	130	130
130	130	130	130
130	130	130	130

280

Figure 2b

130	130	130	130

270

Figure 2a

Figure 3

START — 401

PROMPT USER FOR
AUTHENTICATION — 402

AUTHENTICATION
GOOD — 403

no

405 — THREE
ATTEMPTS

no

yes

yes

406 — SHUT DOWN
COMPUTER

COMPLETE BOOT
PROCESS — 404

END

END
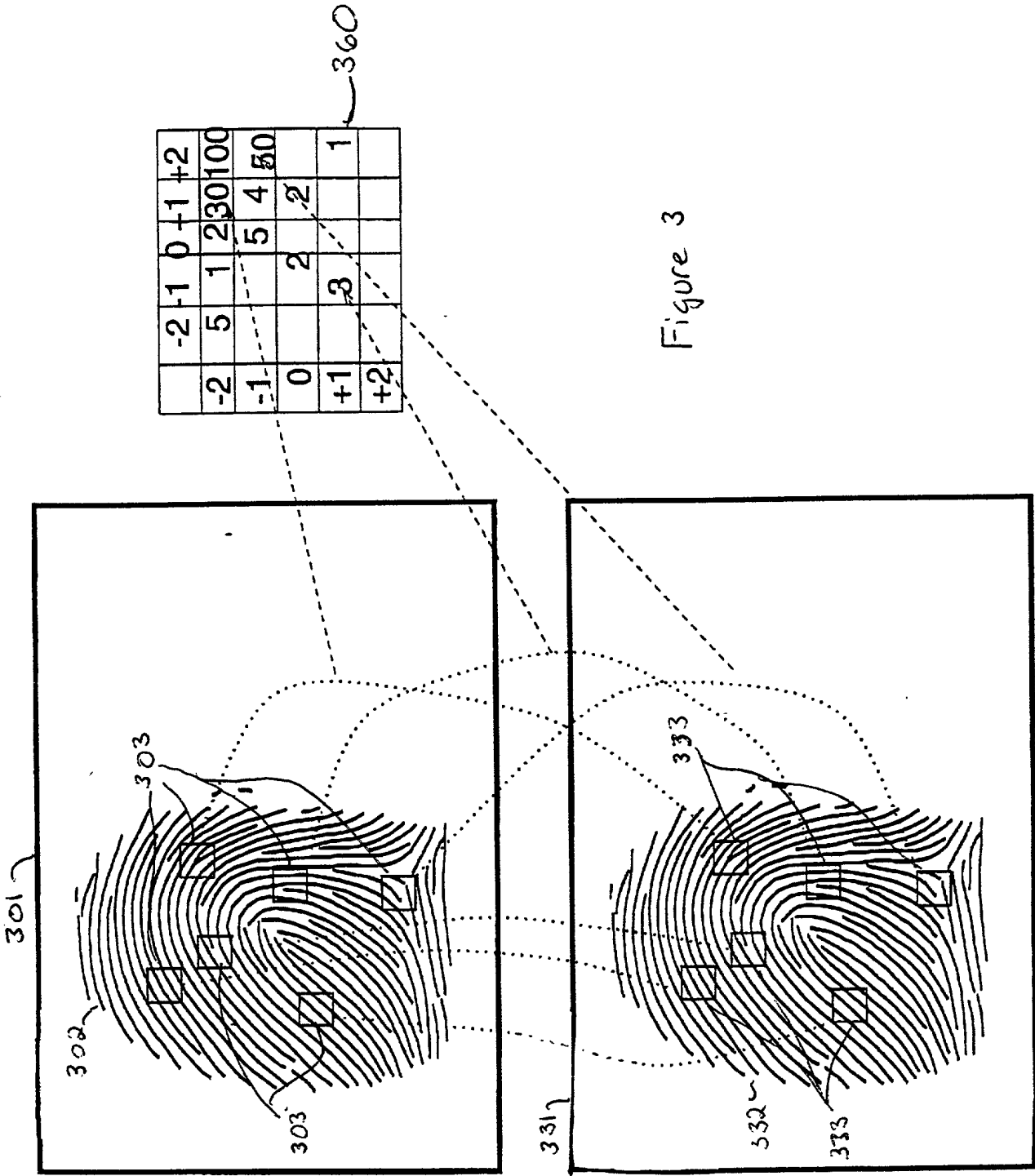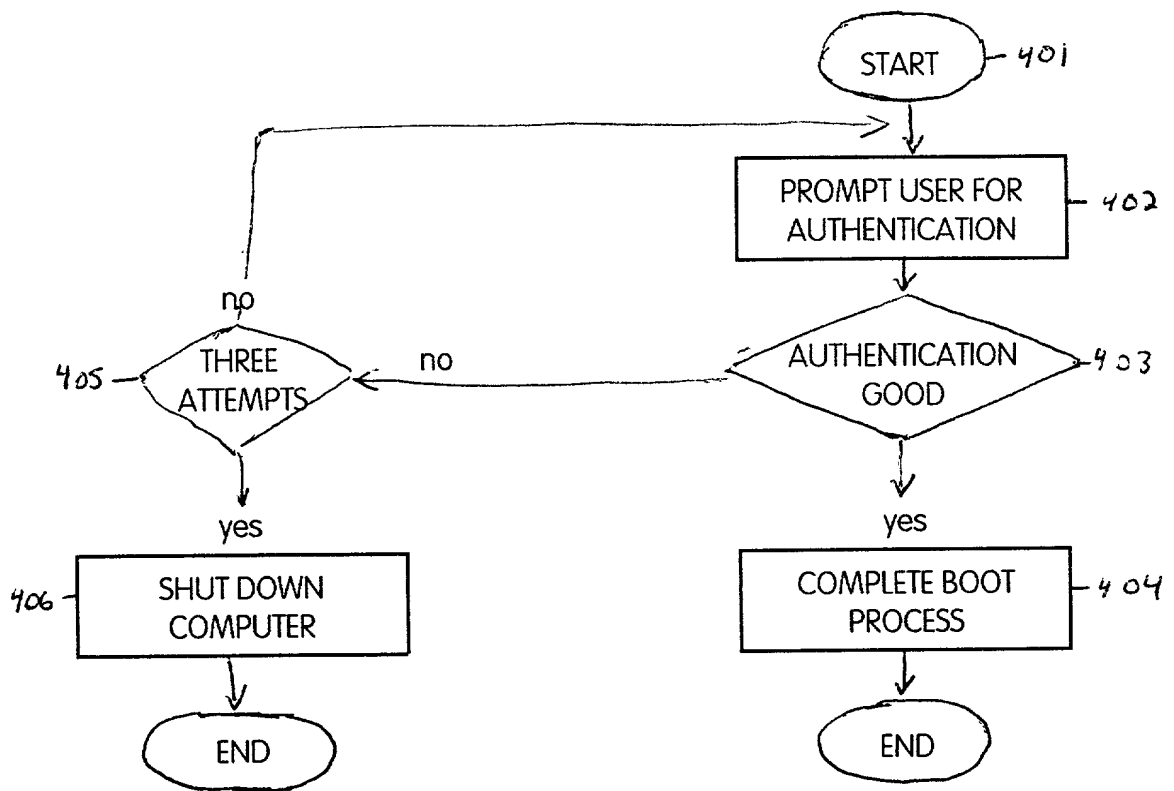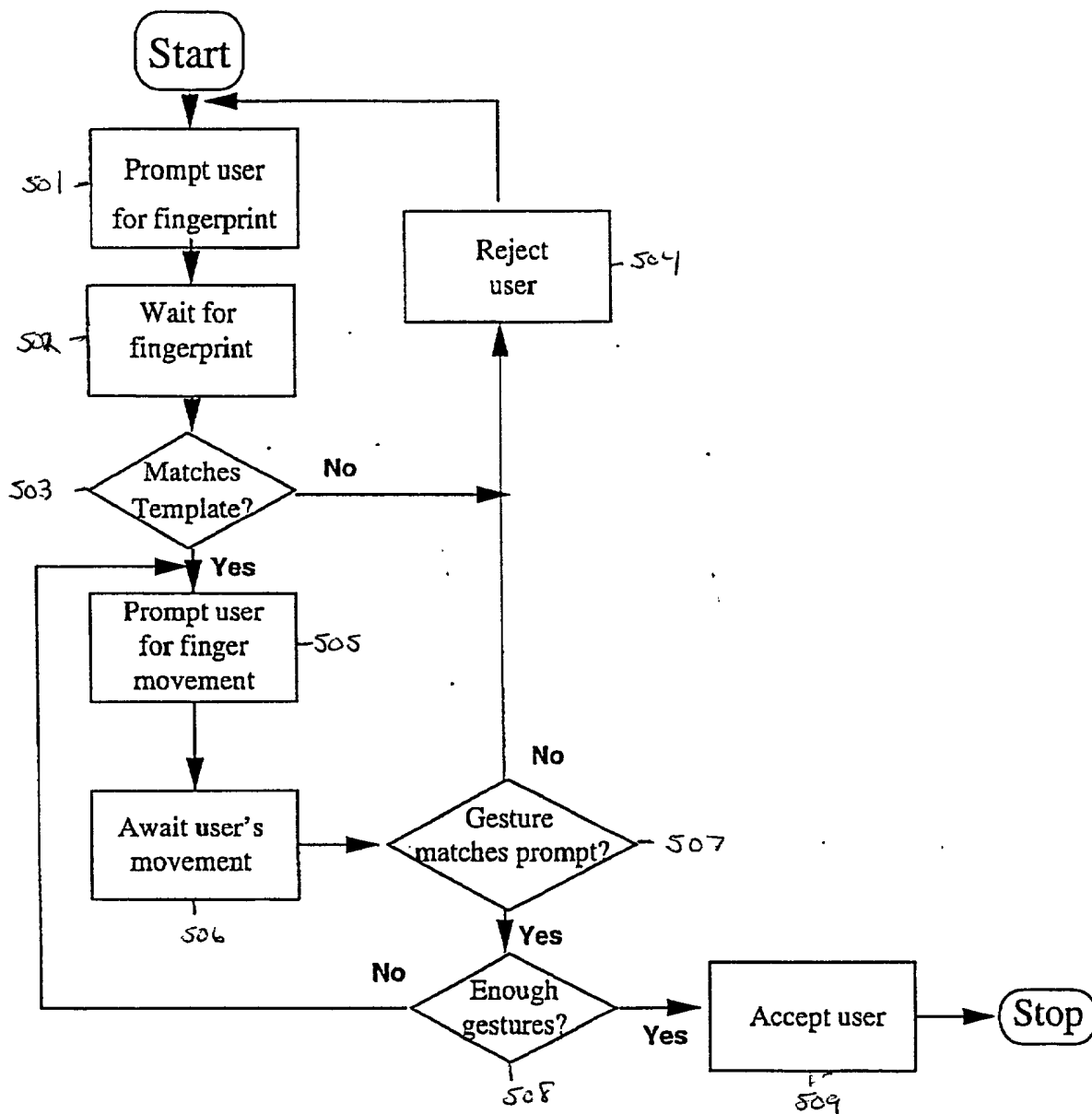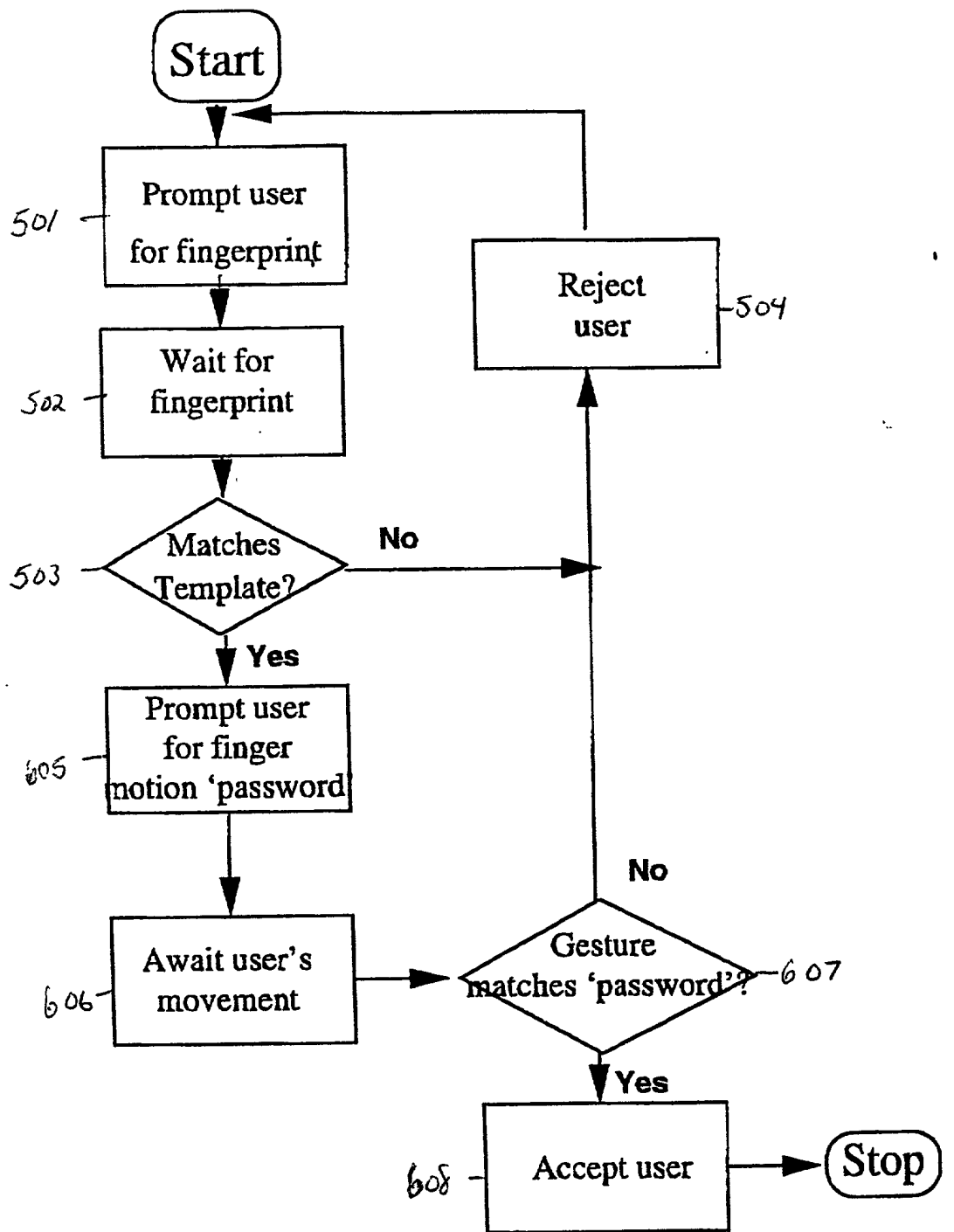
FIGURE 4

Figure 5

Figure 6

Application for United States Patent
Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

IMPROVEMENTS TO A COMBINED FINGERPRINT ACQUISITION AND CONTROL DEVICE

specification of which:

(check   ☒   is attached hereto
one)
                ☐   was filed on _____ as
                           Application Serial No. _____
                           and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).*

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)   Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	yes	no
(Number)	(Country)	(Day/Month/Year Filed)	yes	no

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

Power of Attorney: As a named inventor, I hereby appoint Manny W. Schecter, Reg. No. 31,722, Terry J. Ilardi, Reg. No. 29,936, Stephen C. Kaufman, Reg. No. 29,551, Louis J. Percello, Reg. No. 33,206, Jay P. Sbrollini, Reg. No. 36,266, Robert M. Trepp, Reg. No. 25,933, Daniel P. Morris, Reg. No. 32,053, Kevin P. Jordan, Reg. No. 40,277, Douglas W. Cameron, Reg. No. 31,596, David M. Shofi, Reg. No. 39,835, Christopher A. Hughes, Reg. No. 26,914, Edward A. Pennington, Reg. No. 32,588, John E. Hoel, Reg. No. 26,279, C. Lamont Whitham, Reg. No. 22,424, Marshall M. Curtis, Reg. No. 33,138, and Michael E. Whitham, Reg. No. 32,635, as attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. All correspondence should be directed to Whitham, Curtis & Whitham, Reston International Center, 11800 Sunrise Valley Drive, Suite 900, Reston, Virginia 20191. Phone calls should be directed to Whitham, Curtis & Whitham, at 703/391-2510. -

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1)   Inventor: Rudolf M. Bolle

        Signature: _____   Date: 21st Jan 2000

        Residence: 85 Nottingham Road, Bedford Hills, New York 10507

        Citizenship: Netherlands

        Post Office Address: same as above

(2)   Inventor: Nalini K. Ratha

        Signature: _____   Date: 21st Jan, 2000

        Residence: 14 Granada Crescent, Apt. #17, White Plains, New York 10603

        Citizenship: India

        Post Office Address: same as above

(3)   Inventor: Andrew Senior

        Signature: _____   Date: 21st Jan 2000.

        Residence: 864 West End Avenue, Apartment 4B, New York, New York 10025-4960

        Citizenship: British

        Post Office Address: same as above

*Title 37, Code of Federal Regulations, §1.56(a):

(a) A duty of candor and good faith toward the Patent and Trademark Office rests on the inventor, on each attorney or agent who prepares or prosecutes the application and on every other individual who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application. All such individuals have a duty to disclose to the Office information they are aware of which is material to the examination of the application. Such information is material where there is substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent. The duty is commensurate with the degree of involvement in the preparation or prosecution of the application.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and (1) it establishes, by itself or in combination with other information, a prima facie case of unpatentability; or (2) it refutes, or is inconsistent with, a position the applicant takes in: (i) opposing an argument of unpatentability relied on by the Office, or (ii) asserting an argument of patentability.